

(12)根据专利合作条约(PCT)公布的国际申请。
(‘W’ rldo “IPrOPert”)

国际局。



(10)国际出版物编号 WO 2020/060606 A1。

(43)国际出版日期。

2020 年 3 月 26 日(26.03.2020)WI P O I PCT。

(51)国际专利分类:

G06Q 20/06(2012.01)G06Q 30/02(2012.01)。
G06Q 20/32(2012.01)G06N3/08(2006.01)。
H04L 9/32(2006.01)。

(21) 国际申请编号:

%/美国 20 19/038084。

(22) 国际申请日期:

2019 年 6 月 20 日(20.06.2019 年)。

(25) 备案语言:

英语。

(26) 出版物语言:

英语。

(30)优先级数据:

16/138, 5 18 2018 年 9 月 21 日(21.09.2018)美国。

(71)申请人: 微软技术许可有限责任公司[美国/美国]; One Microsoft Way, 华盛顿州雷蒙德, 98052-6399(美国)。

(72)发明人: 微软技术许可有限责任公司, One Microsoft Way, 华盛顿州雷蒙德, 98052-6399(美国)。微软技术许可有限责任公司, One Microsoft Way, 华盛顿州雷蒙德, 98052-6399(美国)。微软技术许可有限责任公司, One Microsoft Way, 华盛顿州雷蒙德, 98052-6399(美国)。

(74)代理: 微软技术许可有限责任公司, One Microsoft Way, 华盛顿州雷蒙德市, 98052-6399(美国)。

(81)指定国家(除非另有说明, 否则适用于所有可获得的国家保护)。AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, Hu, ID, IL, IN, IR, IS, JO, JP, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, Hu, ID, IL, IN, IR, IS, JO, JP, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW,

(54)职称: 使用身体活动数据的加密货币系统。

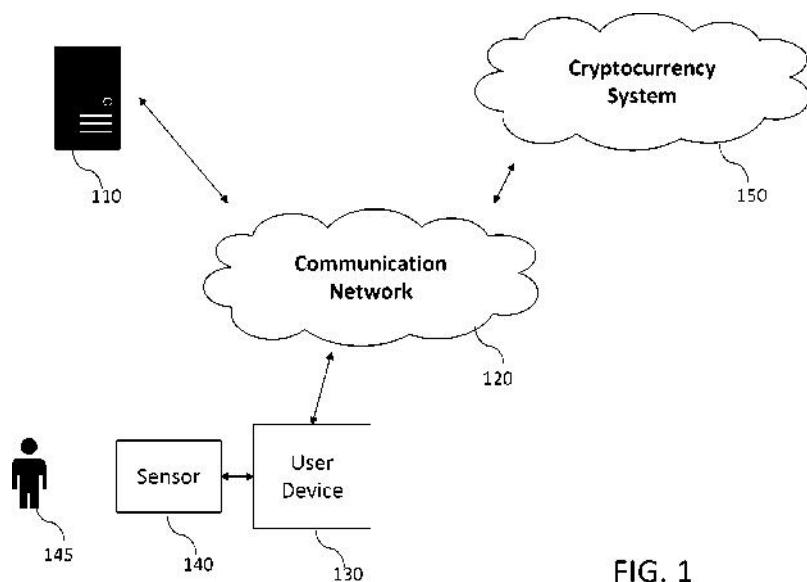


FIG. 1

100 个。

(57)摘要: 可以在加密货币系统的挖掘过程中使用与提供给用户的任务相关联的人体活动。服务器可以向通信地耦合到服务器的用户设备提供任务。通信地耦合到用户的设备或包括在用户的设备中的传感器可以感测用户的身体活动。可以基于感测到的用户的身体活动来生成身体活动数据。通信地耦合到用户的设备的加密货币系统可以验证主体活动数据是否满足由加密货币系统设置的一个或多个条件, 并将加密货币奖励给其主体活动数据被验证的用户。

SC、SD、SE、SG、SK、SL、SM、ST、SV、SY、TH、TJ、TM、TN、TR、TT、TZ、UA、UG、US、UZ、VC、VN、ZA、ZM、ZW。

WO 2020/060606 铝|。

(84)指定国家(除非另有说明, 对于可用的每一种f区域保护): ARIPO(BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚(AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲(AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, Hu, IE, TR)、OAPI(BF、BJ、CF、CG、CI、CM、GA、GN、GQ、GW、KM、ML、MR、NE、SN、TD、TG)。

规则 4.17 下的声明:

- 申请人申请和获批予专利的权利(规则第 4.17(H)条)。
- 关于申请人要求优先于在先申请的权利(规则 4.17(Hi))。

发表:

- 与国际检索报告(第 21 条第(3)款)。

使用身体活动数据的加密货币系统。

背景。

[0001]虚拟货币(也称为数字货币)通常是通过互联网实现的交换媒介,不与特定的政府支持的“平面”
5 (印刷)货币(如美元或欧元)捆绑在一起,通常设计为允许即时交易和无国界的所有权转移。虚拟货
个。
币的一个例子是加密货币,其中加密被用来保护交易并控制新单元的创建。

[0002]存在多种加密货币。其中,最广为人知的是基于区块链的加密货币。大多数基于区块链的加
密货币都是去中心化的,因为它没有中央控制点。然而,基于区块链的加密货币也可以在具有对加
密货币的中央控制点的集中式系统中实现。比特币是基于区块链的加密货币的例子之一。2008年,
10 中本聪(Satoshi Nakamoto)在一篇名为《比特币:一个点对点的电子现金系统“。

个。
[0003]区块链是存储交易列表的数据结构,可被视为记录源标识符和目的地标识符之间的交易的分
布式电子分类账。事务被捆绑到块中,并且每个块(第一个块除外)都指向或链接到区块链中的前一
个块。计算机资源(或节点等)。维护区块链并以密码方式验证每个新区块以及相应区块中包含的事
务。这个验证过程包括通过计算解决一个也很容易验证的难题,有时被称为“工作证明
15 (Proof-of-Work)”。这个过程被称为“挖掘”。挖掘可能是一个概率很低的随机过程,因此需要进
个。
行大量的试错才能解决一个计算困难的问题。因此,采矿可能需要巨大的计算能量。

[0004]关于这些和其他一般考虑,描述了以下实施例。此外,虽然已经讨论了相对具体的问题,但
是应该理解,实施例不应局限于解决背景中识别的具体问题。

摘要。

20 [0005]本公开的一些示例性实施例可以使用与提供给用户的任务相关联的人体活动作为在。
个。

25
个。

30
个。

加密货币系统。例如，当用户执行由信息或服务提供商提供的任务(例如查看广告或使用某些互联网服务)时从用户发射的脑波或体温可以用于挖掘过程。基于用户的身体活动产生的数据可以作为工作证明，而不是一些传统的加密货币系统所需要的大量计算工作，因此，用户可以在不知不
觉中解决计算困难的问题。因此，本公开的某些示例性实施例可以降低挖掘过程的计算能量，并
5 使挖掘过程更快。
个。

[0006]本文提供了用于使用人体活动数据的加密货币系统的计算机可读存储介质的系统、方法和硬件方面。根据本公开的各种实施例，服务器可以向通信地耦合到服务器的用户的设备提供任务。通信地耦合到用户的设备或包括在用户的设备中的传感器可以感测用户的身体活动。可以基于感测到的用户的身体活动来生成身体活动数据。通信地耦合到用户的设备的加密货币系统可以验证身体活
10 动数据是否满足由加密货币系统设置的一个或多个条件，并将加密货币奖励给其身体活动数据被验
个。证的用户。

[0007]示例被实现为计算机进程、计算系统或诸如设备、计算机程序产品或计算机可读介质的制品。根据一个方面，计算机程序产品是计算机系统可读的计算机存储介质，并且对包括用于执行计算机进程的指令的计算机程序进行编码。

15 [0008]提供本概要是为了以简化形式介绍一组概念，这些概念将在下面的详细描述中进一步描述。
个。本概要不打算识别所要求保护的主题的关键特征或基本特征，也不打算用于限制所要求保护的主题的范围。

附图的简要说明。

[0009]将参照附图描述根据本公开的各种实施例，其中：

20 [0010]图 1..1 示出了其中可以实践本公开的一些示例性实施例的示例性环境；
个。
[0011]图 1..2 显示了一个分散的加密货币系统的系统图，根据。

25
个。

30
个。

涉及本公开的示例性实施例；

[0012]图 3。3 示出了根据本公开的示例性实施例的计算机实现的方法的流程图；

[0013]图 3。4 示出根据本公开的示例性实施例的用于生成身体活动数据的操作的流程图；

[0014]图 1。5 示出了根据本公开的示例性实施例的用于验证身体活动数据的操作的流程图；

⁵
个。[0015]图 3。6 示出根据本公开的示例性实施例的区块链和区块链的两个示例性块；

[0016]图 1。图 7 示出了根据本公开的另一个示例性实施例的使用矢量或嵌入的计算机实现的方法的流程图。8 示出了其中可以实现此描述的系统、方法和计算机程序产品中涉及的进程的计算机或处理系统的示例性框图。

[0018]除非另有说明，否则不同附图中相应的数字和符号通常指的是相应的部件。附图是为了清楚¹⁰地说明实施例的相关方面而绘制的，并且不一定是按比例绘制的。
个。

实施例的详细描述。

[0019]在下面的详细描述中，参考形成其一部分的附图，并且附图中以图解的方式示出了可以实施本发明的具体实施例。对这些实施例进行了足够详细的描述，以使本领域的技术人员能够实践本发明，并且应当理解，可以利用其他实施例，并且可以在不背离本发明的精神和范围的情况下进行结构、逻辑和电气改变。因此，下面的详细描述不是在限制意义上进行的，并且本发明的范围仅由所¹⁵附权利要求及其等价物限定。附图中相同的数字表示相同的部件，这从使用上下文中应该是显而易见的。

[0020]术语“加密货币”可以指一种数字货币，其中加密技术被用来管理货币单位的生成和验证资金的转移。许多加密货币包括使用区块链来提供安全和防止欺诈，作为重复支出。本公开的一些实²⁰施例可以在区块链之外的替代加密货币机制中使用。这里描述的系统、方法和计算机程序产品可以个。应用于集中式和。

²⁵
个。

³⁰
个。

分散的加密货币网络或数据库。

[0021]图 2。1 示出了其中可以实践本公开的一些示例性实施例的示例性环境 100。示例环境 100 包括但不限于任务服务器 110、通信网络 120、用户设备 130、传感器 140 和密码货币系统 150 中的至少一个。

5 个。[0022]任务服务器 110 可以通过通信网络 120 向用户设备 130 提供一个或多个任务。例如，任务服务器 110 可以是递送或提供网页的 web 服务器、处理用户与应用或数据库之间的应用操作的应用服务器、云服务器、数据库服务器、文件服务器、服务服务器、实现游戏或游戏服务的游戏服务器、以及递送诸如流视频或音频的媒体的媒体服务器中的至少一个。下面将更详细地讨论由任务服务器 110 提供的任务。

10 个。[0023]或者，加密货币系统 150 可以向用户设备 130 提供一个或多个任务。例如，在分散的加密货币网络中，任务可以由挖掘器(例如，图中的计算资源或节点 210)向用户设备 130 建议。2)。在另一示例中，在集中式加密货币系统中，加密货币服务器可以将任务发送到用户设备 130。

[0024]通信网络 120 可以包括任何有线或无线连接、互联网或任何其他形式的通信。尽管在图 1 中标识了一个网络 120。1 中，通信网络 120 可以包括图 1 中所示的任何服务器、设备、资源和系统之 15 个。间的任意数量的不同通信网络。1 和 2 和/或这里描述的其他服务器、设备、资源和系统。通信网络 120 可以实现各种计算资源或设备、服务器和系统之间的通信。通信网络 120 的各种实现可以采用不同类型的网络，例如但不限于计算机网络、电信网络(例如，蜂窝)、移动无线数据网络、以及这些和/或其他网络的任意组合。

[0025]用户设备 130 可以包括能够处理和存储数据/信息并通过通信网络 120 进行通信的任何设备。20 例如，用户设备 130 可以包括个人计算机、服务器、蜂窝电话、平板电脑、膝上型计算机、智能设备(例如，智能手表或智能电视)。图 1 中示出了用户设备 130 的示例性实施例。6.。

[0026]传感器 140 可以被配置成感测用户 145 的身体活动。如图 2 所示。1，传感器 140 可以是与用户设备 130 分开的组件。

25 个。

30 个。

和/或通信地连接到用户设备 130。或者，传感器 140 可以包括并集成在用户设备 130 中。例如，用户设备 130 可以是其中具有传感器 140 的可感知设备。传感器 140 可以向用户设备 130 发送信息/数据。传感器 140 可以包括例如但不限于功能性磁共振成像(FMRI)扫描仪或传感器、脑电图(EEG)传感器、近红外光谱(NIRS)传感器、心率监视器、热传感器、光学传感器、射频(RF)传感器、
5 超声波传感器、照相机或可以测量或感测身体活动或扫描人体的任何其他传感器或扫描仪。例如，

功能磁共振成像可以通过检测与血流相关的变化来测量身体活动。功能磁共振成像可以使用磁场和无线电波来创建身体的详细图像(例如，大脑中的血液流动来检测活动区域)。 材料。

(Http://news.berkely.edu/2011/09/22/brain-movies/)。显示了 fMRI 如何测量与视觉信息相关的大脑活动并生成图像数据的一个示例。

10 [0027] 加密货币系统 150 可以包括用于处理命令的一个或多个处理器以及存储一个或多个加密货币数据结构中的信息的一个或多个存储器。在一些实施例中，加密货币系统 150 可以是集中式加密货币系统或网络，例如但不限于，可以由第三方实体或运行任务服务器 110 的同一实体私有运行的服务器。在其他实施例中，加密货币系统 150 可以是公共可访问的网络系统(例如，分布式分散计算系统)。
5 [0028] 例如，如图所示，加密货币系统 150 可以是包括一个或多个计算资源 210 的分散式网络 200，例如分散式区块链网络。2. 在图 2 的实施例中。2，可能没有控制加密货币网络 200 的中央机构。区块链网络 200 上存储的数据(即公共分类账)可能不会全部存储在中心位置。区块链网络 200 可以包括用于处理命令的多个处理器和以一个或多个区块链数据结构存储信息的多个存储器。区块链网络 200 可以维护连续增长的数据块列表的一个或多个区块链，其中每个数据块指的是其列表上
20 的先前块。要求每个区块引用区块链中的所有先前区块，从而产生区块链，该区块链被硬化以防止篡改和修订，从而区块链中存储的信息是不可变的。

[0029] 计算资源 210 可以包括已经加入区块链网络 200 并在区块链网络 200 中形成阳极的任何设备、计算机、系统或其他。算出。

25 个。

30 个。

资源 210 可以包括例如但不限于个人计算机、服务器、蜂窝电话、平板电脑、膝上型计算机、智能设备(例如智能手表或智能电视)或能够通过通信网络 120 存储信息和通信的任何其他设备。在一些实施例中，计算资源 210 可以彼此独立或未知，其中例如计算资源 210 保持匿名。每个计算资源 210 可以包括存储区块链网络 200 的公共分类账 230 的至少一部分的副本的存储器 220。
5 计算资源 210 还可以执行一个或多个程序以执行与维护区块链网络 200 相关联的各种功能，包括例如更新公共分类账 230、生成新块或任何其他类似功能。

[0030]为了说明起见，图 3..1 示出未包括在区块链网络 200 中的用户设备 130。然而，用户设备 130 可以是区块链网络 200 的一部分，并且被实现为图中的计算资源 210 之一。2.

[0031]公共分类帐 230 可以存储通过区块链网络 200 执行的任何交易，包括但不限于例如与区块链
10 网络 200 相关并在区块链网络 200 上发生的任何交易。因为每个计算资源 210 存储区块链网络 200 个。的公共分类帐 230 的至少一部分的副本，所以可以在任何时间通过比较存储的多个计算资源 210 的副本来独立地验证公共分类帐 230 的准确性。

[0032]计算资源 210 之间通信可以通过通信网络 120 进行。图 2 的通信网络 120。2 可以是与图 2 的通信 120 相同的网络，也可以是与图 2 的通信 120 不同的网络。1.. 在一些实施例中，每个计算资
15 源 210 可以直接与其他计算资源 210 通信。在一些实施例中，一些计算资源 210 可能不能彼此直接个。通信。例如，它们没有连接到相同的通信网络 120。在这种情况下，计算资源 210 之间与区块链网络 200 相关的通信可以通过使用剩余计算资源 210 中的一个或多个作为中介来发生。在一些实施例中，一个或多个计算资源 210 可能不会一直保持到区块链网络 200 的连续连接。例如，计算资源 210 可以仅在每天的特定时间段期间连接到区块链网络 200，或者可以仅全间歇性地连接到区块链网
20 络 200。由于区块链网络 200 的分散性质，由一个或多个计算资源 210 进行的这种间歇连接不会影个。响区块链网络 200 的整体操作，因为公共分类帐 230 的副本存储在多个。

25
个。

30
个。

计算资源 210。一旦断开的计算资源 210 重新连接到区块链网络 200，断开的计算资源 210 就可以从已经连接到区块链网络 200 的一个或多个计算资源 210 接收公共分类账 210 的更新副本。

[0033]图 3..3 示出了根据本公开的示例性实施例的计算机实现的方法的流程图。

[0034]方法 300 开始于图 310 所示的操作 310。其中任务服务器 110 通过通信网络 120 向用户 145 的 5 个设备 130 提供一个或多个任务。任务包括，例如但不限于，观看或收听信息(例如，广告)一定时间、使用服务(例如，搜索引擎、聊天机器人、电子邮件、社交媒体/联网服务以及任何互联网或网络服务)、将信息/数据上传或发送到网站、服务器或网络(例如，内容共享网站、云网络或服务器)、或可能对用户产生影响的任何其他信息或服务。在区块链中，任务可以作为交易包括在公共分类账 230 中。

10 个。[0035]此外，由任务服务器 110 提供的一个或多个任务可以包括解决用于区分人和机器输入使得人而不是计算机能够通过它的测试，诸如区分计算机和 Flumans 的计算机自动化程序(CAPTCHA)和旨在确定计算机用户是人类的类似 CAPTCHA 的系统 ReCAPTCHA。该任务可以要求用户 145 解决验证挑战，例如但不限于基于图像的挑战，该挑战包括提示用户 145 通过与一个或多个图像交互来解决该挑战的指令。

15 个。[0036]在操作 320，当用户 145 执行由任务服务器 110 提供的任务时或之后，传感器 140 可以感测用户 145 的身体活动，该身体活动是与由任务服务器 110 提供的任务相关的身体响应，然后将感测到的用户 145 的身体活动发送到用户设备 130。身体活动可以包括例如但不限于从人体发射的辐射、脑活动、体液流动(例如，血液流动)、器官活动或运动、身体运动、以及可以由图像、波、信号、文本、数字、度数或任何形式的信息或数据来感知和表示的任何其他活动。人体辐射的例子可 20 个。能包括身体的辐射热、脉搏频率或脑波。脑波可以包括，例如，但不限于，(I)涉及学习或记忆任务的伽马波，(II)涉及逻辑思维和/或有意识思维的 β 波，(III)可能与潜意识思维有关的阿尔法波，(IV)可能与深沉和原始情绪有关的 θ 波，(V)可能涉及睡眠或深度放松的三角波，或(VI)。

25 个。

30 个。

脑电图(EEG)，可以用来评估大脑中的电活动，如深度集中。身体运动的例子可以包括眼睛运动、面部运动或任何其他肌肉运动。此外，使用功能磁共振成像可以感觉到大脑活动。功能磁共振成像通过检测与血流相关的变化来测量大脑活动。这项技术依赖于脑血流和神经元激活相耦合的事实。当大脑的某个区域在使用时，流向该区域的血流量也会增加。

5 个。**[0037]**在操作 330，用户设备 130 基于传感器 140 感测到的身体活动生成身体活动数据。操作 330 可以是挖掘过程的一部分，该挖掘过程是用于解决计算困难问题的过程。图 3 中示出了操作 330 的一个示例性实施例。4.。如图所示。4，操作 330 可以包括操作 410 和 420。

10 个。**[0038]**在操作 410，可以将传感器 140 感测到的身体活动编码为符号形式，例如字母、数字、符号和包括字符序列的字符串。在一个示例中，可以通过从感测到的身体活动中提取一个或多个值来编码
10 个。身体活动，例如身体活动信号的最小和/或最大幅度或频率(例如，脑电波)。在另一示例中，用户设备 130 可以对感测到的身体活动随时间开窗并采样，并计算采样值的平均值。在又一示例中，用户设备 130 可以生成身体活动的原始数据。在又一示例中，在操作 420，用户设备 130 可以使用一个或多个滤波器来过滤身体活动的原始信号，以将过滤后的身体活动信号应用于音频散列函数或算法。或者，与人体活动相关联的任何统计值都可以从传感器 140 感测到的身体活动编码。

15 个。**[0039]**在操作 420，可以通过使用诸如散列算法或函数的加密算法将编码的主体活动转换为加密输出。例如，散列函数包括映射输出数据集的初始输入数据集的函数。通常，散列函数可以是可用于将任意大小的数据映射到固定大小的数据的任何函数。散列函数允许人们轻松地验证某些输入数据是否映射到给定的散列值，但是如果输入数据是未知的，则故意难以通过知道存储的散列值来重建它(或任何等效的备选方案)。散列算法或函数可以包括在加密货币系统或数据库的挖掘软件或程序中。
20 个。**[0040]**例如，操作 420 可以使用音频散列函数，其中对编码的身体活动的频率的直方图求和，或者使用比特操作，诸如异或。

25 个。

30 个。

对编码的身体活动执行具有下一个或素数模数的每个直方图桶的函数。

[0041]在一些实施例中，可以使用其中主体活动本身是散列的模拟散列函数。例如，由传感器 140 感测到的波或信号，例如但不限于来自 EEG 传感器的 α 、 β 、 δ 或伽马波，可以使用变换算法或公式(例如快速傅立叶变换(FFT)或可以卷积、相加或乘以波或信号以产生直方图的任何其他算法或公式)变换为直方图。⁵ 散列可以是直方图本身。例如，散列可以是 FFT 的输出，其中每个分量是频带，并且值是对应于每个频带的计数。在另一示例中，例如，如果存在不容易发生的某种统计保证，则期望的属性可以是前两个频率直方图尽可能接近于零。

[0042]然而，操作 420 是可选的。在某些实施例中，用户设备 130 可以在不加密或散列编码主体活动的情况下将在操作 410 生成的编码主体活动发送到加密货币系统 150。¹⁰

[0043]尽管图 4 所示的。¹⁰ 3 示出了包括操作 410 和 420 的操作 330 由用户设备 130 处理，操作 410 和 420 中的至少一个可以由另一个(或多个)设备、服务器、资源或系统(例如任务服务器 110、密码货币系统 150 或任何其他服务器)处理。例如，用户设备 130 可以生成感测到的身体活动的原始数据，将其发送到密码货币系统 150、任务服务器 110 或任何其他服务器，然后密码货币系统 150、任务服务器 110 或任何其他服务器可以对感测到的身体活动的原始数据进行编码或散列。⁵

[0044]回过头来参照图 2。¹⁵ 3，在操作 340，加密货币系统 150 验证由用户设备 130 生成的用户 145 的身体活动数据是否满足由加密货币系统 150 的算法设置的一个或多个条件。可以通过模拟可以构成散列的所有身体活动上的人体活动来设置条件。机器学习算法可用于模拟身体活动并设置有效身体活动的条件，例如但不限于使用生成性对抗性网络。²⁰

[0045]在一些实施例中，加密货币系统 150 验证用户 145 的身体活动数据(例如，在操作 410 产生的身体活动的代码或在操作 420 产生的身体活动的散列)²⁵ 是否可以表示用户 145 的身体活动在目标范围内。可以使用用户 145 执行由任务服务器 110 提供的任务所需的认知努力量来确定目标范围。例如，为了验证用户 145 的主体活动的散列，加密货币系统 150。

25
个。

30
个。

可以确定例如但不限于(I)用户 145 的主体活动的散列是否具有由加密货币系统 150 设置的特定特定模式、重复模式、数学属性或前导数字、字符或串(例如前导零)的数量，或者(Ii)用户 145 的主体活动的散列是否小于当前目标值。加密货币系统 150 设置的数字模式的示例可以是散列的第一特定数字形成质数的模式，或者通过将散列的第一特定数字应用于预设公式而计算出的数字形成质⁵数的模式(例如，通过将预定数字或由加密货币系统 150 设置的数字加或减到散列的前四位而计算出的数字形成质数)。重复数字模式可以包括重复数字(例如，前导 0、散列中间的 1、散列的最后四位数字中的两个、以及散列中包括的任何重复数字)和重复数字序列(例如，前导重复数字对，例如“121212”，或三元组“123123”)。如果用户 145 的身体活动的散列具有期望的模式或在目标范围内，则认为工作证明或赌注证明已解决，并且该散列可以是新的块。可以周期性地改变目标范围或¹⁰值以保持预先选择的难度水平，尽管这不是必需的。例如，目标值可能与难度成反比。通过改变难度，可以保持大致恒定的块生成速率。

[0046]可以使用统计数据设置有效身体活动的目标范围，从而不能验证正常身体活动、容易发生的活动或假冒身体活动。例如，有效身体活动的目标范围可以从人类矿工不能伪造他们自己的身体活动以满足目标范围以证明和验证工作证明的范围中选择。

¹⁵ [0047]此外，操作 340 处的验证可以包括过滤掉无效任务、格式错误的数据(语法错误)或从未授权用户发送的或由机器学习系统生成的数据。例如，加密货币系统 150 可以从用户设备 130 接收在应用散列算法之前生成的身体活动的数据，对该数据进行重新散列，然后将重新散列的数据与从用户设备 130 接收到的散列进行比较，以检查身体活动数据是否是基于人类而不是随机计算机生成的数据生成的。FMRI 的图像的体素可以是在应用散列算法之前生成的身体活动数据的示例。

²⁰ [0048]图 3 中示出了操作 340 的一个示例性实施例。5. 在操作 510，加密货币系统 150 可以检查从。
个。

²⁵
个。

³⁰
个。

用户设备 130 在由加密货币系统 150 设置的目标范围内，或者包括由加密货币系统 150 设置的所需模式。如果主体活动的散列在目标范围内或者具有由加密货币系统 150 设置的期望模式，则加密货币系统 150 将在应用散列算法之前生成的主体活动的数据与来自用户设备 130 的主体活动的散列一起重新散列(操作 520)，然后将重新散列的数据与从用户设备 130 接收的主体活动的散列进行比较(操作 530)。⁵ 如果重新散列的数据与从用户设备 130 接收的主体活动的散列相同，则密码货币系统 150 前进到操作 350。然而，如果在操作 510 中确定主体活动数据的散列超出目标范围或者不包括由加密货币系统 150 设置的期望模式，或者如果在操作 530 中确定重新散列的数据与主体活动的散列不匹配，则可以继续操作 310 或 320。

[0049]在操作 350，当从用户设备 130 发送的身体活动数据满足由加密货币系统 150 设置的一个或多个¹⁰条件时，加密货币系统 150 将加密货币授予用户 145。例如，加密货币系统 150 向用户 145 奖励对应于用户 145 完成的任务的加密货币量。另外，加密货币系统 150 可以将加密货币奖励给任务服务器 110 的所有者或操作员，作为提供诸如搜索引擎、聊天机器人、应用或网站的服务、向用户免费提供对付费内容(例如，视频和音频流或电子书)的访问、或与用户共享信息或数据的奖励。

[0050]例如，在区块链加密货币系统中，在操作 340，图 340 的计算资源 210 中的至少一个。¹⁵ 验证用户 145 的身体活动数据的散列是否有效。在操作 350，当在操作 340 验证用户 145 的身体活动数据的散列时，图 3 的计算资源 210。² 可以向区块链添加新的区块。新块可以包含分配给用户地址的加密货币单元的数量。具有附加添加的区块的新区块链在加密货币网络 150 周围广播。执行操作 340 和 350 的计算资源 210 还可以获得交易费和/或加密货币奖励。

[0051]图 3。²⁰ 图 5 描绘了根据本公开的示例性实施例的区块链 500 和区块链 500 的两个示例性块 510、520。通常，“区块链”被理解为包括一系列块的数据结构，其中每个块包括对应于一个或多个事务的数据，这些数据与链接数据(例如前一个块的散列)一起散列。在本公开的实施例中，交易可以是由用户 145 执行的任务。链条可以。

25
个。

30
个。

然后用于创建分类帐，该分类帐通常是一个仅附加的数据库。一旦将数据输入到链的块中，该条目基本上是不可反驳的，因为对数据的任何篡改都会反映在链式散列计算中，因此很容易被检测到。**[0052]**区块链 500 可以表示可公开分发的交易分类账，例如图中的分类账 230。2，并且可以包括多个块。诸如块 510 和块 520 的每个块可以包括关于最近事务的数据。例如，由用户 145 执行 5 个的任务和授予用户 145 的加密货币单位的数量，和/或将一个块 520 链接到前一块 510 的链接数据的内容，以及确保区块链 500 的状态有效并且被记录保存系统的大多数认可/验证的工作证明数据，例如，主体活动的经验证的散列。区块链 500 的块 520 的示例性实施例可以包括当前散列、先前块 510 的先前散列、事务。前一个散列是来自前一个块的散列，这确保每个块都与前一个块固定地绑定在一起。前一块 510 的散列可以包括在块 520 中，从而将块 520 链接到前一块 510。

10 **[0053]**在没有计算资源 210 中的至少一个注意的情况下，不能修改交易信息，因此，可以信任区块链 500 来验证在区块链 500 上发生的交易。

[0054]在一些实施例中，向量或嵌入可以用于身体活动数据。插图。7 示出了使用矢量(或嵌入)的计算机实现的方法的示例性实施例的流程图。如上面参照图 3 详细描述的。任务服务器 110 或加密货币系统/网络 150(例如中央加密货币服务器或计算资源(或节点)210)可以执行操作 310，其中通过通信网络 120 向用户设备 130 提出一个或多个任务，并且传感器 140 可以执行操作 320，其中传感器 140 感测或测量用户 145 的身体活动。传感器 140(或用户设备 130)可以以图像、波形、信号、数字、字符、字符串或可以表示身体活动的任何其他形式来生成身体活动的数据。15

[0055]在操作 710，用户设备 130 从传感器 140(或用户设备 130)生成的身体活动的数据产生一个或多个向量(或嵌入)，诸如浮点数数组。存储在用户设备 130 或通过通信网络 120 以通信方式连接到用 20 户设备 130 的任何设备、服务器、系统或网络中的算法可以将传感器 140(或用户设备 130)生成的身体活动的数据转换成一个或多个向量。例如，大脑图像。

25
个。

30
个。

由 fMRI 扫描仪生成的数据可以被馈送到计算机视觉机器学习算法中，例如但不限于卷积神经网络，并且机器学习算法可以从脑图像的一个或多个体素生成一个或多个向量。在一些实施例中，可以在操作 710 处生成一个单个向量。在其他实施例中，当用户 145 正在执行任务时，可以通过随时间采样来产生一系列矢量。身体活动(例如，脑图像的体素)和/或矢量(或嵌入)的数据可以生成 5 个工作证明，并被发送到加密货币系统/网络 150。

[0056]此外，向量可任选地包括与任务相关的一个或多个向量，例如但不限于用户 145 使用或标识用户 145 查看的广告的搜索项。

[0057]在操作 720，可以通过使用加密算法(例如散列算法或函数)将在操作 710 生成的向量转换为加密输出，如以上参考图的操作 420 所解释的。4. 例如，可以使用诸如安全散列算法(SHA)-1、SHA-256、10 SHA-384、SHA-512 和消息摘要(MD)-5 之类的散列算法将向量散列为字节。 15

[0058]然而，操作 720 是可选的。在一些实施例中，用户设备 130 可以将在操作 710 产生的身体活动的向量发送到加密货币系统 150，而不对其进行加密或散列。

[0059]在操作 730，密码货币系统 150 从用户设备 130 接收用户 145 的身体活动的数据(例如，脑图像的体素)和/或用户 145 的身体活动的向量(或散列)。

15 个。[0060]在操作 740，加密货币系统 150 检查从用户设备 130 接收的向量是否具有由加密货币系统/网络 150 设置的一个或多个数学属性。例如，加密货币系统 150 可以确定身体活动的一个或多个向量是否与由加密货币系统 150 的算法设置的合法向量(或基线向量)具有相似性(或关系)。可以使用例如但不限于余弦相似性、欧几里德距离、曼哈顿距离、明可夫斯基距离和贾卡德相似性来测量或计算相似性。可以基于执行相同任务的人的身体活动向量具有一定程度的相似性的假设来设置合法向量。 20 加密货币系统 150，诸如图中的中央加密货币服务器/网络或计算资源(或节点)210。2、可以确定合法向量和相似度。例如，挖掘器喜欢图 210 的计算资源(或节点)210。2 可以分享他们的证据。

25 个。

30 个。

例如，包括但不限于，身体活动的向量，与加密货币网络 150 进行比较，并通过计算工作证明的平均值(例如，矢量和标准偏差的质心或加权平均值)。

[0061]如果从用户设备 130 接收的向量具有由加密货币系统/网络 150 设置的数学属性，则加密货币系统/网络 150 对从用户设备 130 发送的主体活动的数据进行重新散列(操作 750)，然后将重新散列⁵输出与从用户设备 130 接收的向量(或散列)进行比较(操作 760)。例如图 2 的计算机资源(或节点)210。2 可以将从用户设备 130 发送的 fMRI 体素重新散列为向量，然后将重新散列的向量与从用户设备 130 接收的向量进行比较，以检查身体活动数据是否是基于人类而不是随机计算机生成的数据生成的。如果在操作 740 确定接收到的一个或多个向量用户设备 130 不满足由加密货币系统/网络 150 设置的一个或多个数学属性，或者如果在操作 760 确定重新散列的输出与从用户设备 130 接收¹⁰一个或多个向量(或散列)不匹配，则可以继续操作 310 或 320。

[0062]如果重新散列的输出与从用户设备 130 接收到的向量(或散列)相同，则加密货币系统/网络 150 将加密货币授予用户 145，如以上参照操作 350 详细描述的。例如，在区块链加密货币系统中，诸如图 210 的计算资源(或节点)210 之一的挖掘器。执行主体活动数据验证的 2 可以向区块链添加包括主体活动的数据、向量(或散列)和/或分配给用户地址的加密货币单元的数量的新块，在加密货币网¹⁵络 150 周围广播具有新块的新区块链，并且可以获得交易费和/或加密货币奖励。

[0063]图 3.. 8 示出了示例计算机或处理系统的示意图，其可以实现在本公开的一个实施例中在此描述的任何系统、方法和计算机程序产品，诸如任务服务器 110、用户设备 130、密码货币系统 150 和计算资源 210。该计算机系统仅是合适的处理系统的一个示例，并且不打算建议对在此描述的方法的实施例的使用范围或功能的任何限制。所示的处理系统可以与许多其他通用或专用计算系统环境²⁰或配置一起操作。可能适合使用的公知计算系统、环境和/或配置的示例。

25
个。

30
个。

利用图 1 中所示的处理系统。8 可以包括但不限于个人计算机系统、服务器计算机系统、瘦客户端、胖客户端、手持或膝上型设备、多处理器系统、基于微处理器的系统、机顶盒、可编程消费电子产品、网络 PC、小型机系统、大型计算机系统以及包括任何上述系统或设备的分布式云计算环境等。

5 个。**[0064]**计算机系统可以在由计算机系统执行的诸如程序模块的计算机系统可执行指令的一般上下文中描述。通常，程序模块可以包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、逻辑、数据结构等。该计算机系统可以在分布式云计算环境中实施，在分布式云计算环境中，任务由通过通信网络链接的远程处理设备执行。在分布式云计算环境中，程序模块可以位于本地和远程计算机系统存储介质中，包括存储器存储设备。

10 个。**[0065]**计算机系统 800 的组件可以包括但不限于一个或多个处理器或处理单元 810、系统存储器 820 以及将包括系统存储器 820 的各种系统组件耦合到处理器 810 的总线 830。处理器 810 可以包括执行这里描述的方法的软件模块 815。模块 815 可以被编程到处理器 810 的集成电路中，或者从存储器 820、存储设备 840 或网络 850 或其组合加载。

15 个。**[0066]**总线 830 可以表示若干类型的总线结构中的任何一种或多种，包括存储器总线或存储器控制器、外围总线、加速图形端口以及使用各种总线体系结构中的任何一种的处理器或本地总线。作为示例而非限制，这样的体系结构包括工业标准体系结构(ISA)总线、微通道体系结构(MCA)总线、增强型 ISA(EISA)总线、视频电子标准协会(VESA)局部总线和外围组件互连(PCI)总线。

[0067]计算机系统 800 可以包括各种计算机系统可读介质。这样的介质可以是计算机系统可访问的任何可用介质，并且它可以包括易失性和非易失性介质、可移动和不可移动介质。

20 个。**[0068]**系统存储器 820 可以包括易失性存储器形式的计算机系统可读介质，例如随机存取存储器 (RAM) 和 / 或高速缓冲存储器等。计算机系统 800 还可以包括其他可拆卸 / 不可拆卸易失性 / 不可拆卸易失性 / 不可拆卸。

25 个。

30 个。

易失性计算机系统存储介质。仅作为示例，可以提供存储设备 840 以用于从不可移动、非易失性磁介质(例如，硬盘驱动器)读取和写入到不可移动、非易失性磁介质。尽管未示出，但可以提供用于读取和写入可移动、非易失性磁盘(例如，软盘)的磁盘驱动器，以及用于读取或写入诸如 CD-ROM、DVD-ROM 或其他光学介质的可移动、非易失性光盘的光盘驱动器。在这种情况下，每 5 个。个都可以通过一个或多个数据介质接口连接到总线 630。

[0069]计算机系统 800 还可以与诸如键盘、定点设备、显示器 870 等一个或多个外部设备 860、使用用户能够与计算机系统交互的一个或多个设备、和/或任何设备(例如，网卡、调制解调器等)通信。其使得计算机系统能够与一个或多个其他计算设备通信。这种通信可以通过输入/输出(I/O)接口 880 进行。

10 [0070]此外，计算机系统 800 可以经由网络适配器 855 与一个或多个网络 850 通信，例如局域网(LAN)、通用广域网(WAN)和/或公共网络(例如，因特网)。如图所示，网络适配器 855 通过总线 830 与计算机系统的其他组件通信。应当理解，虽然未示出，但是可以结合计算机系统使用其他硬件和/或软件组件。示例包括但不限于：微码、设备驱动程序、冗余处理单元、外部磁盘驱动器阵列、RAID 系统、磁带驱动器和数据归档存储系统等。

15 [0071]如本领域技术人员将理解的，本公开的各方面可以实现为系统、方法或计算机程序产品。因此，本公开的各方面可以采取完全硬件实施例、完全软件实施例(包括固件、驻留软件、微代码等)的形式。或者是结合了软件和硬件方面的实施例，在此通常可以将其统称为“电路”、“模块”或“系统”。此外，本公开的各方面可以采用包含在其上包含计算机可读程序代码的一个或多个计算机可读介质中的计算机程序产品的形式。

20 [0072]可以利用一个或多个计算机可读介质的任意组合。计算机可读介质可以是计算机可读信号介质或计算机可读存储介质。计算机可读存储介质可以是例如但不限于电子、磁、光、电磁、红外或半导体系统、装置或设备，或前述的任何适当组合。计算机可读存储介质的更具体的示例(非穷举列表)将包括。

25
个。

30
个。

便携式计算机磁盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦除可编程只读存储器(EPROM 或闪存)、便携式光盘只读存储器(CD-ROM)、光存储设备、磁存储设备或上述设备的任何适当组合。在本文档的上下文中，计算机可读存储介质可以是可以包含或存储由指令执行系统、装置或设备使用或结合指令执行系统、装置或设备使用的程序的任何有形介质。

⁵ [0073]计算机可读信号介质可以包括传播的数据信号，其中例如在基带中或作为载波的一部分包含一个。计算机可读程序代码。这样的传播信号可以采取各种形式中的任何一种，包括但不限于电磁、光学或其任何适当的组合。计算机可读信号介质可以是任何计算机可读介质，该计算机可读介质不是计算机可读存储介质，并且可以传送、传播或传输由指令执行系统、装置或设备使用或与指令执行系统、装置或设备结合使用的程序。

¹⁰ [0074]包含在计算机可读介质上的程序代码可以使用任何适当的介质来传输，包括但不限于无线、有线、光缆、RF 等，或者前述的任何适当的组合。

[0075]用于执行本发明各方面的操作的计算机程序代码可以用一种或多种编程语言的任意组合来编写，所述一种或多种编程语言包括诸如 Java、Smalltalk、C++等的面向对象的编程语言和诸如“C”编程语言或类似的编程语言的常规过程编程语言、诸如 Perl、VBS 或类似的语言的脚本语言、和/或诸如 Lisp 和 ML 的函数式语言以及诸如 Prolog 的面向逻辑的语言。程序代码可以完全在用户的计算机上、部分在用户的计算机上、作为独立的软件包、部分在用户的计算机上和部分在远程计算机上或者完全在远程计算机或服务器上执行。在后一种情况下，远程计算机可以通过任何类型的网络(包括局域网(LAN)或广域网(WAN))连接到用户的计算机，或者可以连接到外部计算机(例如，通过使用互联网服务提供商的互联网)。

¹⁵ [0076]参照根据本公开的一些实施例的方法、装置(系统)和计算机程序产品的流程图说明和/或框图来描述本公开的各方面。应当理解，流程图的每个方框和/或方框图以及以下各项的组合。

²⁵
个。

³⁰
个。

流程图和/或框图中的框可以由计算机程序指令实现。这些计算机程序指令可以被提供给通用计算机、专用计算机或其他可编程数据处理设备的处理器以生产机器，使得经由计算机或其他可编程数据处理设备的处理器执行的指令创建用于实现流程图和/或框图块中指定的功能/动作的装置。

[0077]这些计算机程序指令还可以存储在计算机可读介质中，该计算机可读介质可以指导计算机、
5 其他可编程数据处理设备或其他设备以特定方式运行，使得存储在计算机可读介质中的指令产生包括实现流程图和/或框图块中指定的功能/动作的指令的制品。

[0078]计算机程序指令还可以被加载到计算机、其他可编程数据处理设备或其他设备上，以使得在计算机、其他可编程设备或其他设备上执行一系列操作步骤以产生计算机实现的过程，使得在计算机或其他可编程设备上执行的指令提供用于实现流程图和/或框图块中指定的功能/动作的过程。

10 [0079]图中的流程图和框图说明了根据本发明的各种实施例的系统、方法和计算机程序产品的可能实现的体系结构、功能和操作。就此而言，流程图或框图中的每个框可以表示代码的模块、段或部分，其包括用于实现指定逻辑功能的一个或多个可执行指令。还应注意，在一些替代实现中，框中注明的功能可以不按附图中注明的顺序发生。例如，根据所涉及的功能，实际上可以基本上同时执行连续显示的两个块，或者有时可以以相反的顺序执行这些块。还应当注意，框图和/或流程图的
15 每个框以及框图和/或流程图中的框的组合可以由执行指定功能或动作的基于专用硬件的系统或者专用硬件和计算机指令的组合来实现。

[0080]计算机程序产品可以包括使得能够实现此描述的方法的所有相应特征，并且当加载到。

20
个。

25
个。

30
个。

计算机系统--能够执行这些方法。在本上下文中，计算机程序、软件程序、程序或软件指的是一组指令的任何语言、代码或符号的任何表达，该组指令旨在使具有信息处理能力的系统直接或在以下任一项或两项之后执行特定功能：(A)转换为另一种语言、代码或符号；及/或(B)以不同的材料形式复制。

⁵ 个。[0081]这里使用的术语仅用于描述特定实施例，并不意在限制本发明。如本文所使用的，单数形式“a”、“an”和“the”意在也包括复数形式，除非上下文另有明确指示。还应当理解，当在本说明书中使用术语“包括”和/或“包括”时，指定存在所陈述的特征、整数、步骤、操作、元素和/或组件，但不排除存在或添加一个或多个其他特征、整数、步骤、操作、元素、组件和/或它们的组。

¹⁰ 个。[0082]以下权利要求中的所有装置或步骤加功能元件(如果有的话)的相应结构、材料、动作和等价物旨在包括用于结合具体权利要求的其他权利要求元件执行该功能的任何结构、材料或动作。本发明的描述是为了说明和描述的目的而提出的，但并不打算以所公开的形式详尽地或局限于本发明。在不背离本发明的范围和精神的情况下，许多修改和变化对于本领域的普通技术人员将是显而易见的。选择和描述该实施例是为了最好地解释本发明的原理和实际应用，并使本领域普通技术人员能够理
¹⁵ 解具有适合于预期的特定用途的各种修改的各种实施例的本发明。

[0083]本公开的各个方面可以具体化为包含在计算机或机器可用或可读介质中的程序、软件或计算机指令，其使得计算机或机器在计算机、处理器和/或机器上执行时执行该方法的步骤。还提供了一种机器可读的程序存储设备，其有形地包含可由机器执行以执行本公开中描述的各种功能和方法的指令程序。

²⁰ 个。[0084]本公开的系统和方法可以在通用计算机或专用计算机系统上实现和运行。术语“计算机”

²⁵
个。

³⁰
个。

本申请中可以使用的“系统”和“计算机网络”可以包括固定和/或便携式计算机硬件、软件、外围设备和存储设备的各种组合。计算机系统可以包括联网或以其他方式链接以协同执行的多个单独组件，或者可以包括一个或多个独立组件。本申请的计算机系统的硬件和软件组件可以包括并且可以包括在诸如台式机、膝上型计算机和/或服务器的固定和便携式设备内。模块可以是实现某些
5 个。“功能”的设备、软件、程序或系统的组件，其可以体现为软件、硬件、固件、电子电路等。

[0085]虽然已经描述了本发明的具体实施例，但是本领域的技术人员将理解，还有与所描述的实施例等效的其他实施例。因此，应当理解，本发明不受具体说明的实施例的限制，而仅受所附权利要求的范围的限制。

概念。

10 个。[0086]概念 1。一种加密货币系统，包括：一个或多个处理器；以及存储可执行指令的存储器，所述可执行指令如果由所述一个或多个处理器执行，则配置所述加密货币系统以：与用户的设备通信；接收基于所述用户的身体活动生成的身体活动数据，其中所述身体活动由通信耦合到所述用户的设备或包括在所述用户的设备中的传感器感测；验证所述用户的身体活动数据是否满足由所述加密货币系统设置的一个或多个条件；以及将加密货币奖励给其身体活动数据被验证的用户。
15

个。[0087]概念 2。任何在前和/或在后的概念的系统，其中由传感器感测到的身体活动包括从用户发射的身体辐射、体液流动、脑波、脉率或身体热辐射中的至少一个。

[0088]概念 3。该系统具有任何在前和/或在后的概念，其中所述一个或多个条件是基于与提供给用户的设备的任务相关联的人体活动量来设置的。

20 [0089]概念 4。该系统具有任何在前和/或在后的概念，其中所述一个或多个条件包括身体活动数据表
示用户执行提供给用户的设备的任务的条件。

[0090]概念 5。任何在前和/或在后概念的系统，其中身体活动数据是使用散列算法生成的，该散列算法将人体活动转换为。

25 个。

30 个。

加密输出，并且所生成的身体活动数据包括感测到的用户身体活动的散列。

[0091]概念 6。任何在前和/或在后概念的系统，其中身体活动数据包括从传感器感测到的身体活动产生的一个或多个向量。

[0092]概念 7。任何在前和/或在后概念的系统，其中所述一个或多个条件包括主体活动的散列包括重
5 个。复模式或由加密货币系统设置的数学属性的条件。

[0093]概念 8。任何在前和/或在后概念的系统，其中所述加密货币系统通过为所授予的加密货币生成块并将所述块添加到存储在所述加密货币系统中的区块链来将所述加密货币授予所述用户。

[0094]概念 9。该系统包括任何在前和/或在后的概念，其中该块包括数据，该数据包括：提供给用户的设备的任务；关于所授予的加密货币的信息；与主体活动相关联的散列；以及先前块的散列。
10

10 [0095]概念 10。任何在前和/或在后的概念的系统，其中提供给用户的设备的任务包括用于验证设备的用户是否是人类的测试。

[0096]概念 11。根据任何在前和/或在后概念的系统，其中，所述加密货币系统被配置为：从用户的设备接收在应用散列算法之前生成的主体活动的数据和主体活动的散列；对主体活动的数据进行重
15 新散列；以及将重新散列的数据与从用户的设备接收的主体活动的散列进行比较，以验证主体活动
15 个。数据。

[0097]概念 12。一种计算机实现的方法，包括：由耦合到网络的用户的设备通过网络接收任务；由通信地耦合到用户的设备或包括在用户的设备中的传感器感测用户的身体活动；基于感测到的用户的身体活动生成身体活动数据；由通信地耦合到用户的设备的加密货币系统验证身体活动数据是否满足由加密货币系统设置的一个或多个条件；以及由加密货币系统将加密货币授予其身体活动的用
20 户。
20

[0098]概念 13。根据任何在前和/或在后概念的方法，其中由传感器感测到的身体活动包括从以下位置发射的身体辐射中的至少一个。

25
个。

30
个。

使用者，体液流动，脑电波，脉搏频率或身体热辐射。

[0099]概念 14。如前面和/或后面的概念所述的方法，其中所述一个或多个条件由所述加密货币系统基于与提供给所述用户的设备的任务相关联的人体活动量来设置。

[00100]概念 15。如前面和/或后面的概念所述的方法，其中，验证身体活动数据是否满足一个或多
5 个条件包括确定身体活动数据是否表示用户执行提供给用户的设备的任务。

[00101]概念 16。根据任何在前和/或在后概念的方法，其中，验证主体活动数据是否满足一个或多
个条件包括确定主体活动数据是否表示由加密货币系统设置的多于一定数量的主体活动。

[00102]概念 17。根据任何在前和/或在后概念的方法，其中使用将人体活动转换成加密输出的散列
算法来生成身体活动数据，并且所生成的身体活动数据包括感测到的用户的身体活动的散列。

10 [00103]概念 18。任何在前和/或在后的概念的方法，其中身体活动数据包括从传感器感测到的身体
活动产生的一个或多个向量。

[00104]概念 19。根据任何在前和/或在后概念的方法，其中，验证主体活动数据是否满足由加密货币
系统设置的一个或多个条件包括确定感测到的主体活动的散列是否包括重复模式或由加密货币
系统设置的数学属性。

15 [00105]概念 20。如前面和/或后面的概念所述的方法，其中授予加密货币包括由加密货币系统生成
个。用于授予的加密货币的块，并将生成的块添加到存储在加密货币系统中的区块链。

[00106]概念 21。根据任何在前和/或在后概念所述的方法，其中所述块包括数据，所述数据包括：
提供给用户的设备的任务；关于所授予的加密货币的信息；所生成的与主体活动相关联的散列；以
及先前块的散列。

20 [00107]概念 22。根据任何在前和/或在后概念的方法，其中该任务包括用于验证该设备的用户是否
个。是人类的测试。

[00108]概念 23。任何在前和/或在后的概念的方法，

25
个。

30
个。

还包括：由加密货币系统从用户的设备接收在应用散列算法之前生成的主体活动的数据和主体活动的散列；由加密货币系统对主体活动的数据进行重新散列；以及由加密货币系统将重新散列的数据与从用户的设备接收的主体活动的散列进行比较，以验证主体活动数据。

[00109]概念 24。一种设备，包括：通信地耦合到传感器的一个或多个处理器，所述传感器被配置⁵为感测用户的身体活动；以及存储可执行指令的存储器，所述可执行指令如果由所述一个或多个处理器执行，则将所述设备配置为：接收任务；基于所感测的用户的身体活动生成身体活动数据，其中所感知的身体活动与所接收的任务相关联；以及将所生成的身体活动数据发送到验证身体活动数据以奖励加密货币的系统或网络。

[00110]概念 25。任何在前和/或在后的概念的系统，其中由传感器感测到的身体活动包括从用户发¹⁰射的身体辐射、体液流动、脑波、脉率或身体热辐射中的至少一个。

[00111]概念 26。任何在前和/或在后概念的系统，其中使用将人体活动转换成加密输出的散列算法来生成身体活动数据。

[00112]概念 27。任何在前和/或在后概念的系统，其中身体活动数据包括从传感器感测到的身体活动产生的一个或多个向量。

[00113]概念 28。任何在前和/或在后概念的系统，其中，通过从传感器感测到的身体活动产生一个或多个向量并加密该一个或多个向量来生成身体活动数据。¹⁵

20
个。

索赔。

1. 一种加密货币系统，包括：

一个或多个处理器；以及。

存储可执行指令的存储器，如果所述可执行指令由所述一个或多个处理器执行，则将所述加密货币系统配置为：

与用户的设备通信；

接收基于用户的身体活动生成的身体活动数据，其中身体活动由通信地耦合到用户的设备或包括在用户的设备中的传感器感测；

验证用户的身体活动数据是否满足加密货币系统设置的一个或多个条件；以及。

将加密货币奖励给其身体活动数据经过验证的用户。

2. 如权利要求 1 所述的系统，其中由传感器感测到的身体活动包括从用户发射的身体辐射、体液流动、脑波、脉率或身体热辐射中的至少一个。

3. 如权利要求 1 所述的系统，其特征在于，所述一个或多个条件是基于与提供给用户的设备的任务相关联的人体活动量来设置的。

4. 根据权利要求 1-3 之一所述的系统，其中，所述身体活动数据是使用将人体活动转换为加密输出的散列算法生成的，并且所生成的身体活动数据包括感测到的所述用户的身体活动的散列。

5. 根据权利要求 1-3 之一的系统，其中，身体活动数据包括从传感器感测到的身体活动产生的一个或多个向量。

6. 根据权利要求 1-3 之一所述的系统，其中，所述加密货币系统通过为所奖励的加密货币生成块并将所述块添加到存储在所述加密货币系统中的区块链来将所述加密货币授予所述用户。

7. 如权利要求 6 所述的系统，其特征在于，所述块包括数据，所述数据包括：

提供给用户的设备的任务；

有关获奖加密货币的信息；

与身体活动相关联的散列；以及。

上一个块的哈希。

8. 如权利要求 3 所述的系统，其中，提供给用户的设备的任务包括用于验证设备的用户是否是人类的测试。

9. 如权利要求 4 所述的系统，其特征在于，所述加密货币系统被配置为：

从用户的设备接收在应用散列算法之前生成的身体活动的数据和身体活动的散列；

对身体活动的数据进行重新散列；以及。

将重新散列的数据与从用户的设备接收的身体活动的散列进行比较，以验证身体活动数据。

10. 一种计算机实现的方法，包括：

由耦合到网络的用户的设备通过网络接收任务；

由通信耦合到用户的设备或包括在用户的设备中的传感器感测用户的身体活动；

基于感测到的用户的身体活动来生成身体活动数据；

由通信耦合到用户的设备的加密货币系统验证主体活动数据是否满足由加密货币系统设置的一个或多个条件；以及。

由加密货币系统将加密货币授予其身体活动数据被验证的用户。

11. 根据权利要求 10 所述的方法，其中由传感器感测到的身体活动包括从用户发射的身体辐射、体液流动、脑波、脉率或身体热辐射中的至少一个。

12. 如权利要求 10 所述的方法，其特征在于，所述一个或多个条件由所述加密货币系统基于与提供给所述用户的设备的所述任务相关联的人体活动量来设置。

13. 根据权利要求 10-12 之一所述的方法，其中，使用将人体活动转换为加密输出的散列算法来生成身体活动数据，并且所生成的身体活动数据包括感测到的用户的身体活动的散列。

14. 根据权利要求 10-12 之一所述的方法，其中，所述身体活动数据包括从由所述传感器感测到的身体活动产生的一个或多个向量。

15. 根据权利要求 13 所述的方法，还包括：

加密货币系统从用户的设备接收在应用散列算法之前生成的主体活动的数据和主体活动的散列；

由所述加密货币系统对所述主体活动的数据进行重新散列；以及。

加密货币系统将重新散列的数据与从用户的设备接收的主体活动的散列进行比较，以验证主体活动数据。

WO2020/060666 个 / 美国 2019/038084.

1/8

100
个。

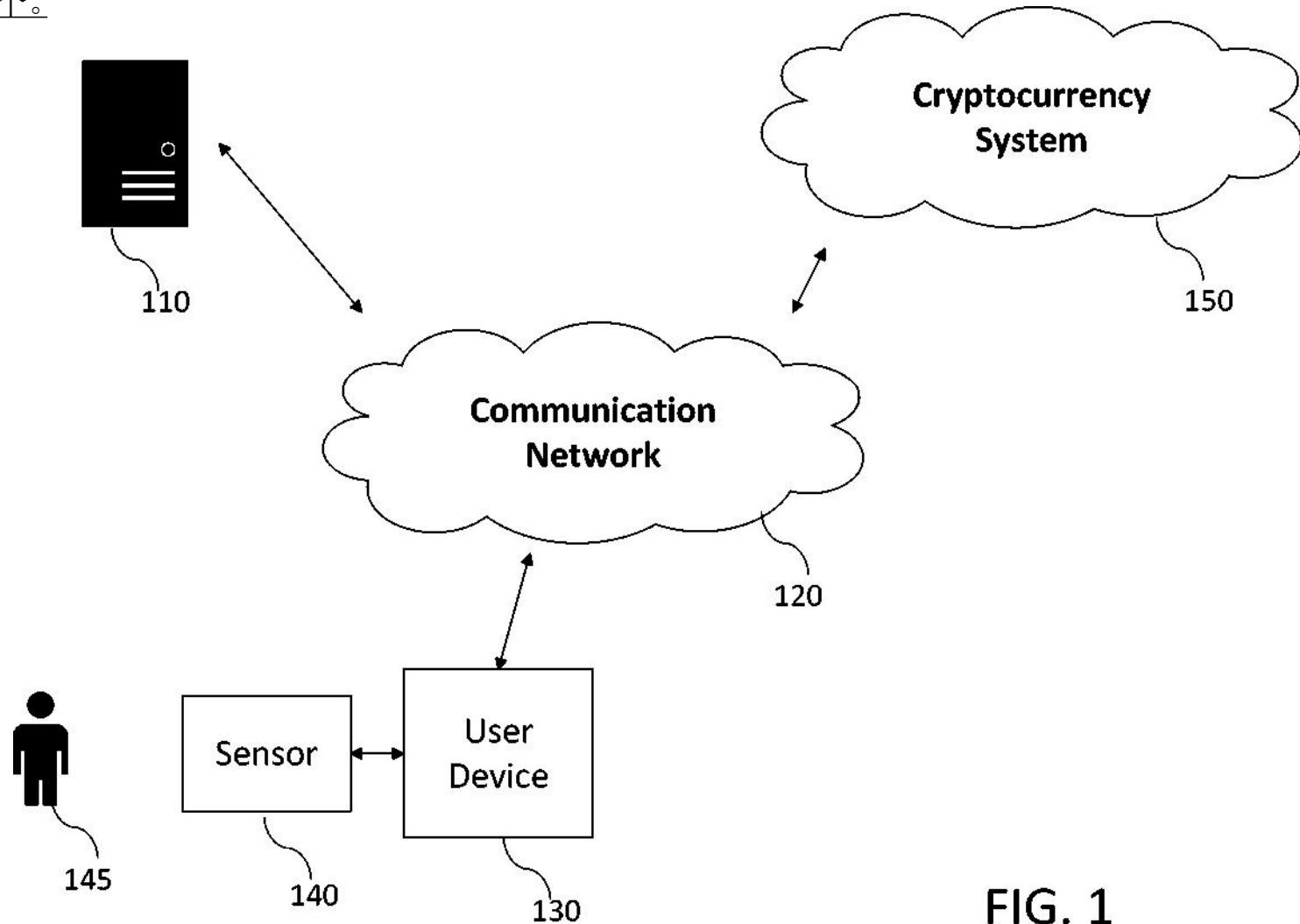


FIG. 1

WO2020/066666 个 / 美国 2019/038084.

2/8

200(150)

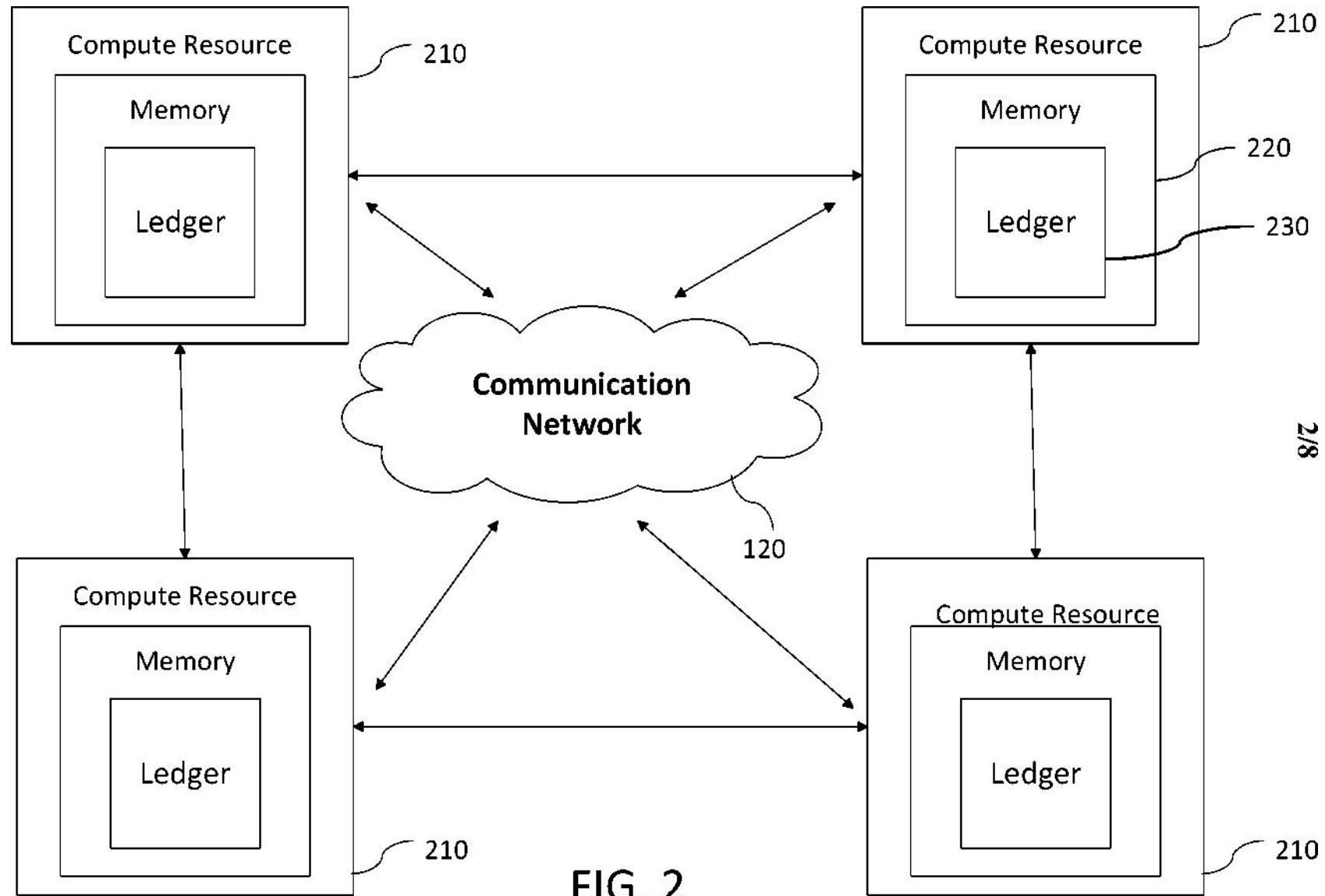
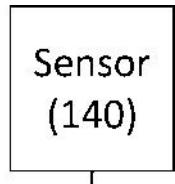
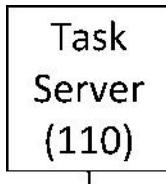


FIG. 2

300 个。

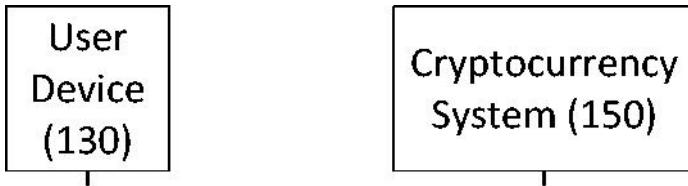


提供任务。

三百一十。感知用户。
我。
身体活动。

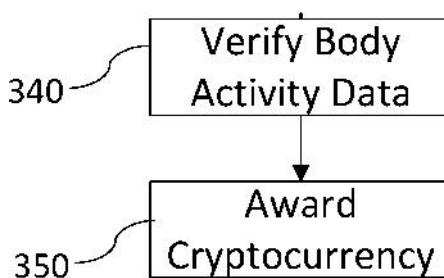
插图。3
个。

W
O
20
20
/0
60
60
6个 / 美国
20
19
/0
38
08
4。



三百二十。我。——
生成实体。
活动数据。

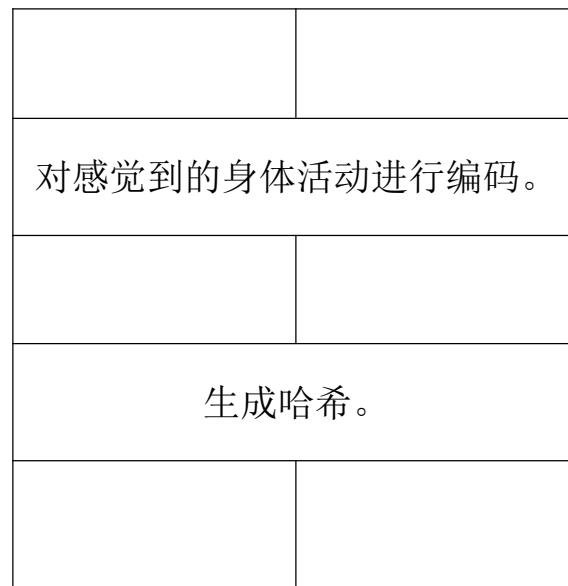
三百三十。



W
O
20
20
/0
60
60
6 个 / 美国
20
19
/0
38
08
4。

4-
。
00
。

四百一十。
四百二十。

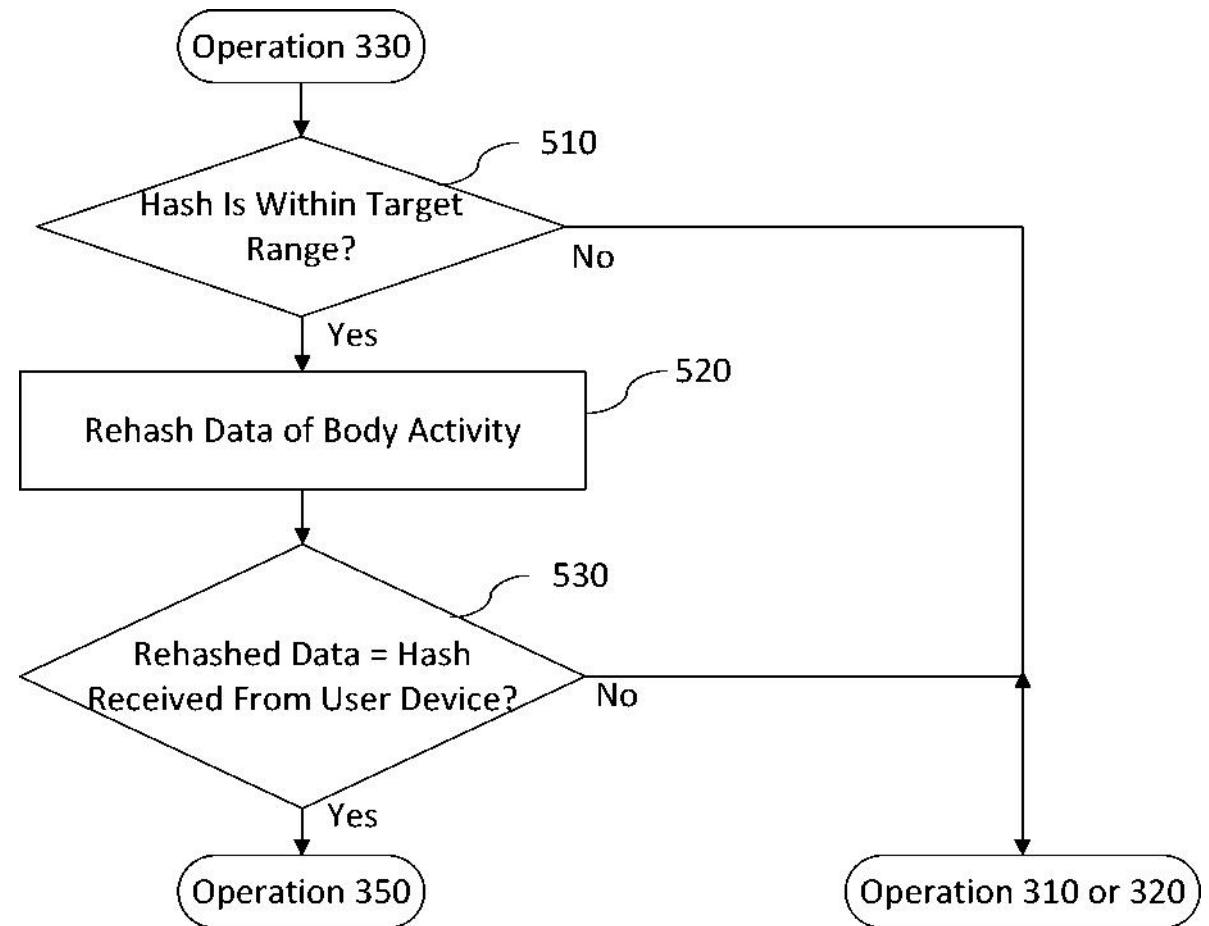


三百三十。

插图。

4.。

WO2020/06666个/美国2019/038084。



插图。5
个。

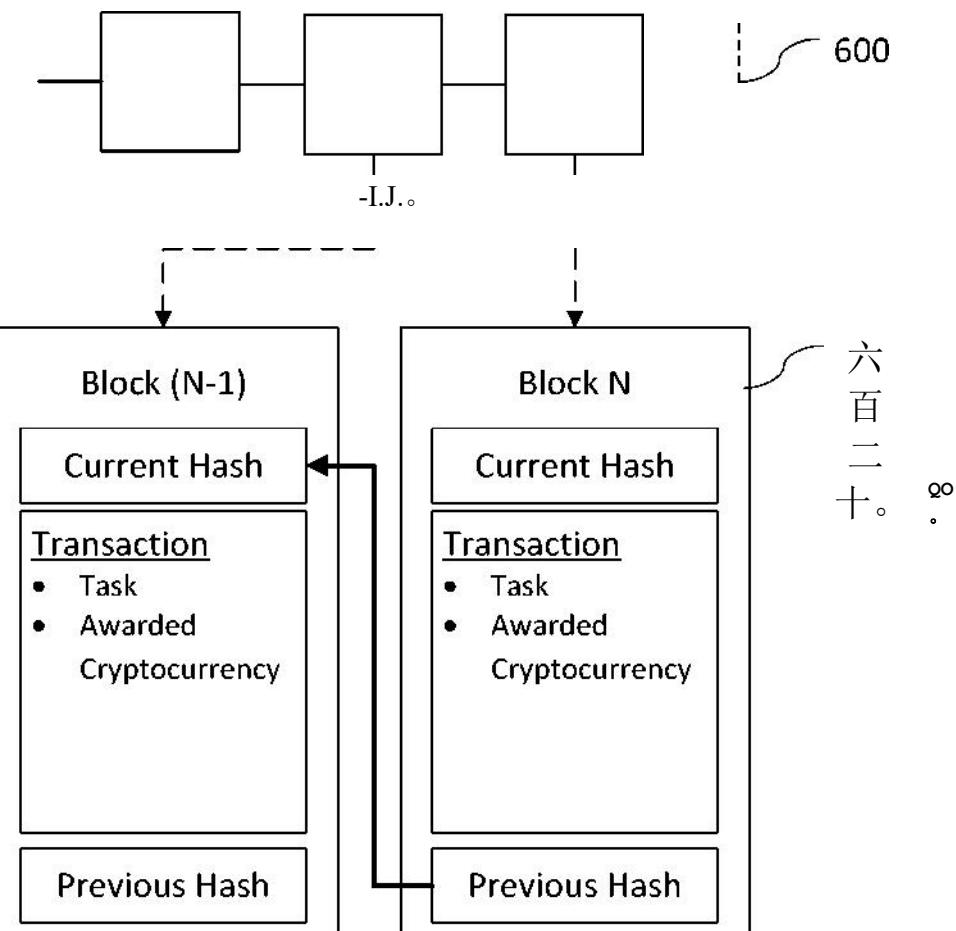
六

百

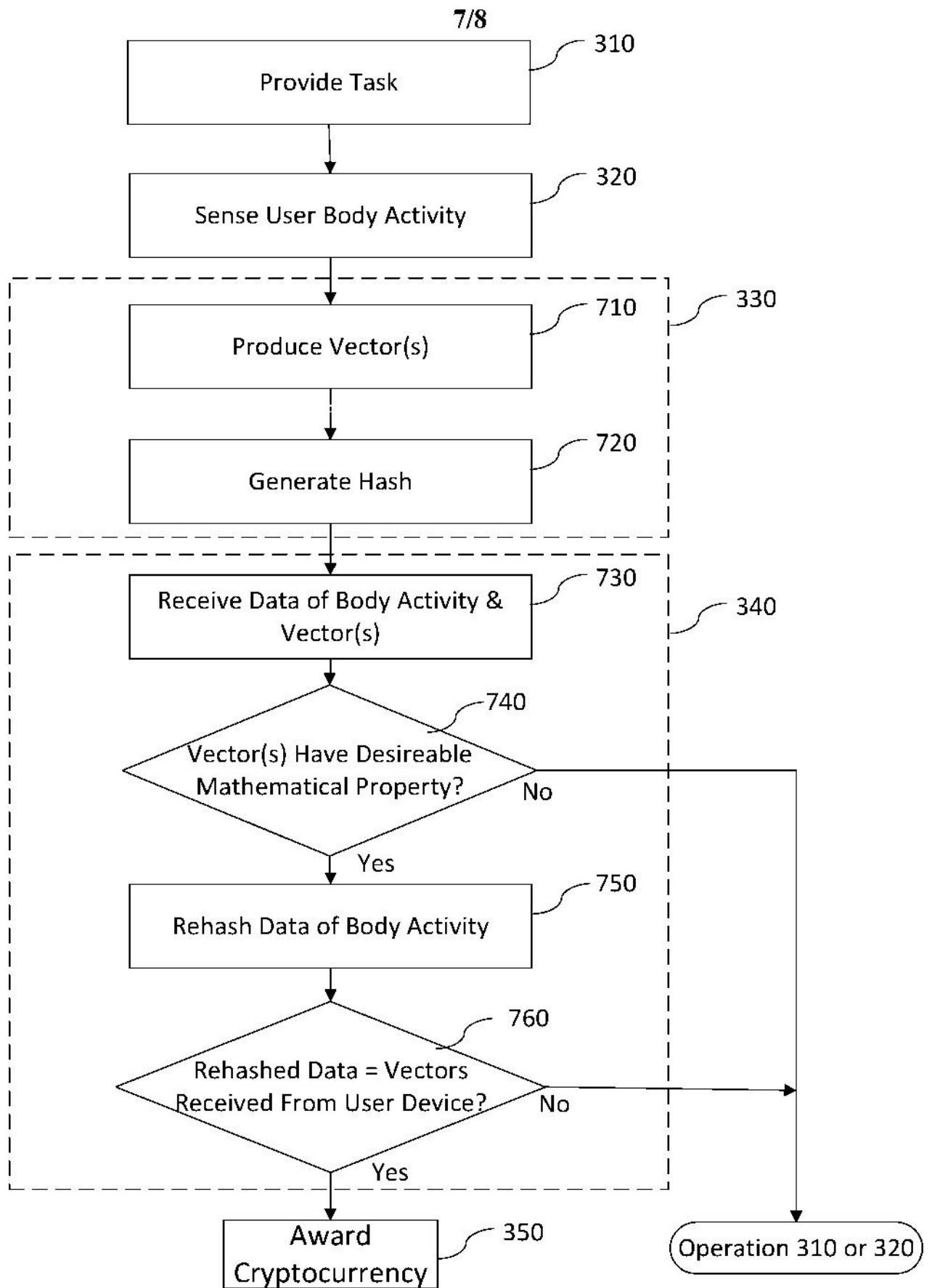
—→

十。

W
O
20
20
/0
60
60
6 个 / 美国
20
19
/0
38
08
4。

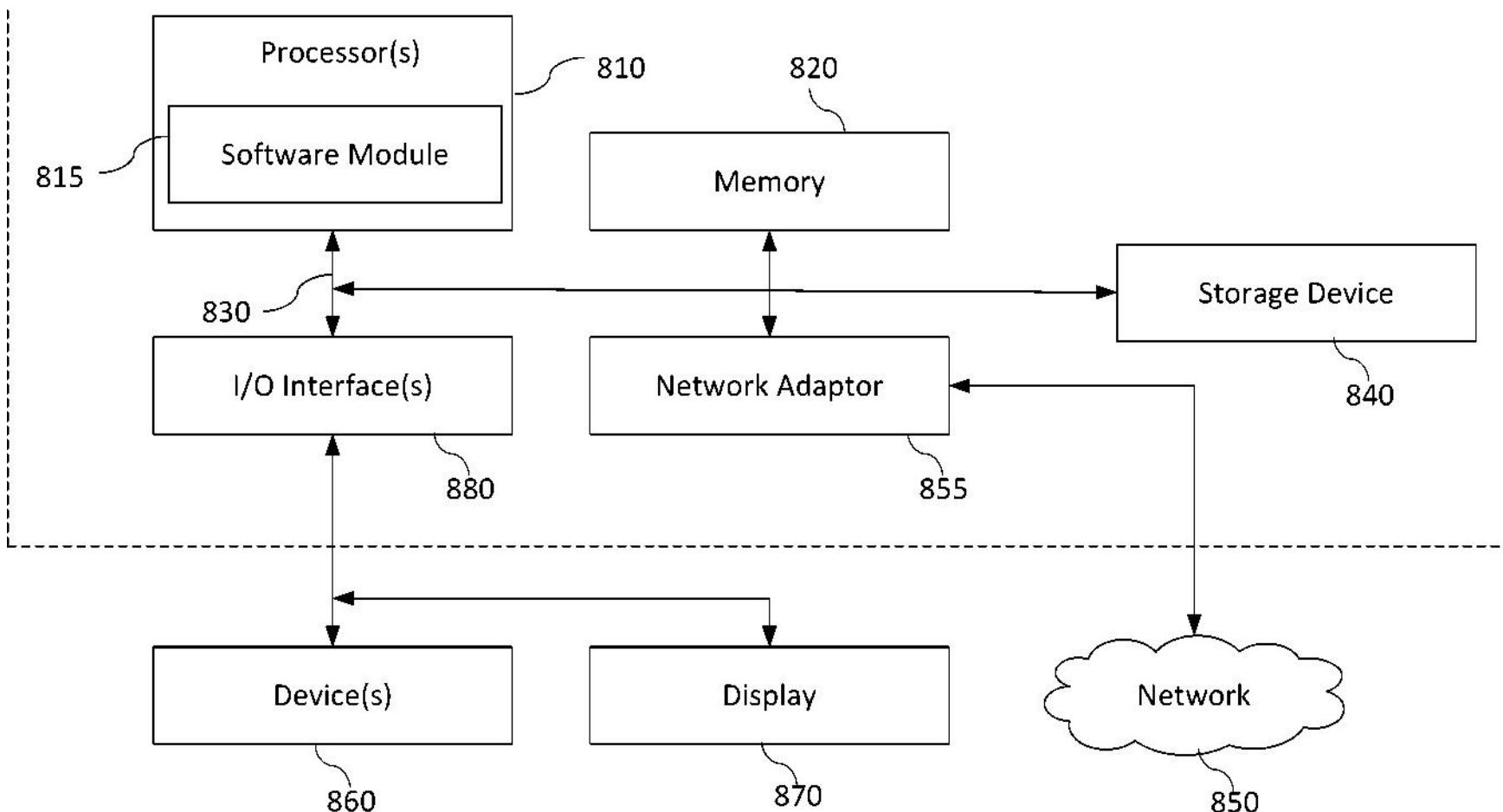


插
图。6
个。



插图。7个。

八
百。



插
图。8
个。

国际搜索报告。

国际申请号。

%/美国 20 19/038084。

A. 浅谈亚物质的分类。

我不知道。

添加。

G06Q20/06 G06Q20/32 H04L9/32 G06Q30/02 G06N3/08。

根据国际专利分类(IPC)或同时适用于国家分类和 IPC。

B. 搜索的字段。

搜索的最少文档(分类系统后跟分类符号)。

G06Q H04 L G07G G06N

搜索的文档(最低文档除外), 只要此类文档包括在搜索的字段中。

国际检索期间查阅的电子数据库(数据库名称和可行时使用的检索词)。

类别。一	引述文件, 并在适当情况下注明有关段落。	与索赔编号相关。
X.	<p>Neuroress et AL: “通过神经接口 NeuroGRESS 实现机电系统控制”, 2018 年 2 月 8 日(2018-02-08), XP055612926, 从互联网检索: 网 址 : iHttps://s3.eu-central-1.amazonaws.com/ 。 costar-whitePapers/d525e659fddaebecll8647 4abc02142360577982f85787d1086372blf0668f4c O.pdf。 [检索于 2019-08-14]全文。</p> <p>-/-。</p>	1-15。

EPO-Interterna I, WPI 数据。

C. 被视为有关的文件。

—被引用文献的特殊类别。

定义不被认为特别相关的现有技术的一般状态的“A”文件。

E “较早的申请或专利, 但在国际申请日或之后发表。

可能对优先权要求提出质疑的“L”文件, 或被引用以确定另一引文的发表日期或其他特殊原因(指定的)的“L”文件。

指口头披露、使用、展示或其他方式的“O”文件。

在国际申请日期之前但晚于要求的优先权日期发布的“P”文件。

国际搜索报告。

在国际申请日期或优先权日期之后发表的、与申请没有冲突的、但被引用以理解本发明背后的原理或理论的“T”以后的文件。

具有特殊相关性的“X”文档；要求保护的发明不能被认为是新颖的，或者当文档单独使用时不能被认为涉及创造性步骤。

实际完成国际搜索的日期。

2019年8月14日。

ISA/的名称和邮寄地址。

欧洲专利局，P.B。5818 Patentlaan 2 NL-2280 HV Rijswijk 电话：
(+31-70)340-2040，传真：(+31-70)340-3016。

表格 PCT/ISA/210(第二页)(2005年4月)。

当该文档与一个或多个其他这样的文档组合时，所要求保护的发明不能被认为涉及创造性步骤，这种组合对本领域技术人员来说是显而易见的。
%7美国 2019/038084。

同一专利家族的文件成员。

国际检索报告邮寄日期。

2019年08月27

日。

获授权人员。

国际搜索报告。

国际申请号。

%/美国 2019/038084。

C(续)。被视为有关的文件。

类别*。	引述文件，并在适当情况下注明有关段落。	与索赔编号相关。
X。	<p>丽莎·巴里克：“研究人员帮助数字货币用户通过锻炼获得更多奖励”， 2017年8月14日(2017-08-14), XP055613045, 从互联网检索： 网址: https://warwick.ac.uk/newsandevents/pressrelease/Research_Help_Digital/[检索于 2019-08-14]整个文档。</p>	1-15。
一个。	US 2018 年/247191 A1(Katz Randall M[US]et AL)2018 年 8 月 30 日(2018 年 8 月 8 日至 30 日)第[0069]段-第[0124]段。	1-15。

国际搜索报告。

关于专利家族成员的信息。

国际申请号。

%/美国 2019/038084

检索报告中引用的专利文献。	出版日期。	专利家族成员。	出版日期。
美国 2018247191 A1 30-08-2018 年	美国 2018247191 A1 30-08-2018。	美国 2018341861 A1 29-11-2018 年。 美国 2018373983 A1 27-12-2018 年。 美国 2018373984 A1 27-12-2018 年。	

国际搜索报告。